QSIGN S.R.L.

Prestator de servicii de încredere — Trust Service Provider (TSP)

POLITICA TSA

(TSA Policy & Practice Statement)

SERVICIU DE ÎNCREDERE CALIFICAT

(Mărci Temporale Calificate — Qualified Time-Stamps)

Aplicabil:

- **Crearea mărcilor temporale calificate (art. 42 Reg. (UE) 910/2014)**
- **Verificarea și validarea mărcilor temporale calificate**
- **Operarea unității QSIGN TSA Unit G1 (TSU)**

(conform ETSI EN 319 421 / EN 319 422, RFC 3161 / RFC 5816)

INFORMAȚII DOCUMENT

Element	Valoare
Denumire document	Politica TSA / Trust Service Practice Statement pentru serviciul de marcă temporală calificată
Cod intern	QSIGN-TSA-P-v1.0
Versiune	1.0
Data publicării	06.05.2026
Data intrării în vigoare	06.05.2026
Stare	Aprobat

Element	Valoare
Clasificare	Public
Aprobat de	Policy Management Authority (PMA) — QSIGN S.R.L.
Limba originală	Română (cu termeni tehnici bilingvi RO/EN)
Cadru de structurare	ETSI EN 319 421 v1.3.1 §6–7 (TSA management & policies); RFC 3628; structură compatibilă RFC 3647
Conformitate principală	Reg. (UE) nr. 910/2014 (eIDAS), modificat prin Reg. (UE) 2024/1183 — în special art. 19, 24, 41, 42; Legea nr. 214/2024 privind utilizarea semnăturii electronice, a mărcii temporale și prestarea serviciilor de încredere; Ordinul MEDAT nr. 102/29.01.2026 (Anexa 1 — Procedura de acordare, suspendare și retragere a statutului calificat); ETSI EN 319 401 v3.1.1+ (cerințe generale TSP); ETSI EN 319 421 v1.3.1+ (cerințe TSA); ETSI EN 319 422 v1.1.1+ (profil TSReq/TSResp); RFC 3161, RFC 5816 (Time-Stamp Protocol, ESSCertIDv2); RFC 5905 (NTPv4); RFC 8915 (Network Time Security); ETSI TS 119 312 v1.5.1+ (Cryptographic Suites); ETSI EN 319 403-1 v2.3.1+ (audit conformitate); ISO/IEC 27001 / 27002.

1. Introducere și sferă de aplicare

1.1 Prezentare generală

Prezentul document constituie Politica de Serviciu a Autorității de Marcare Temporală (Time-Stamping Authority Policy) și, în același timp, Codul de Practici al QSIGN S.R.L. (denumit în continuare „QSIGN" sau „TSP") în calitate de prestator de servicii de încredere calificate pentru emiterea de mărci temporale electronice calificate, conform art. 42 din Regulamentul (UE) nr. 910/2014 (eIDAS), modificat și completat prin Regulamentul (UE) 2024/1183. Documentul este redactat conform structurii și cerințelor ETSI EN 319 421 v1.3.1 (Policy and security requirements for Trust Service Providers issuing time-stamps), ETSI EN 319 422 v1.1.1 (Time-stamping protocol and time-stamp profiles), precum și RFC 3161 și RFC 5816 pentru profilul TimeStampToken.

QSIGN S.R.L. este societate comercială română înregistrată la Oficiul Registrului Comerțului sub numărul J2024010825402, având cod unic de înregistrare fiscală 34633481, cu sediul social în București, str. Drumea Rădulescu, nr. 26, sector 4. Reprezentantul legal este administratorul Trandafirescu Alexandru Florin. Datele de contact pentru aspecte legate de prezentul document și pentru relația cu Autoritatea pentru Digitalizarea României (ADR) sunt: e-mail alex@qsign.ro, telefon +40 724 167 333, web https://www.qsign.ro/repository.

Prezentul document este parte integrantă a dosarului de notificare depus la ADR conform Anexei 1 la Ordinul MEDAT nr. 102/29.01.2026, în susținerea cererii (notificării) QSIGN privind obținerea statutului de prestator calificat pentru serviciul de marcă temporală calificată. Documentul îndeplinește cerința art. 5 alin. (2) lit. f) din Anexa 1 la Ordinul MEDAT 102/2026 (link la politici, practici și proceduri) și completează arhitectura tehnică descrisă în documentul-anexă „Arhitectura detaliată a serviciului de încredere" (cod intern: ArhitectPKI), publicat odată cu prezenta.

1.2 Sfera de aplicare

Prezenta Politică TSA acoperă exclusiv serviciul calificat de marcă temporală operat de QSIGN prin unitatea de marcare temporală denumită „QSIGN TSA Unit G1" (TSU). Politica reglementează:

- (i) crearea de mărci temporale calificate, în sensul art. 42 din Reg. (UE) 910/2014, cu efectele juridice de la art. 41 alin. (2) din regulament — prezumție de exactitate a datei și orei pe care le indică și de integritate a datelor cu care aceste dată și oră sunt asociate;
- (ii) verificarea și validarea mărcilor temporale calificate emise de QSIGN, prin punerea la dispoziția părților utilizatoare a certificatului TSU, a CRL-ului aplicabil și, prin extensie, a Trust List naționale (TSL) administrate de ADR;
- (iii) operarea TSU și a infrastructurii de sincronizare cu UTC(k), incluzând managementul cheilor TSU, ceremoniile de generare și retragere, precum și raportarea de incidente.

Serviciile de încredere calificate distincte oferite de QSIGN — emiterea certificatelor calificate de semnătură electronică (QCP-n / QCP-n-qscd), emiterea certificatelor calificate de sigiliu electronic (QCP-l / QCP-l-qscd) și gestionarea semnăturilor/sigiliilor calificate la distanță cu QSCD — fac obiectul unui document distinct (QSIGN-CP-CPS-QC-v1.0), iar serviciile necalificate (avansate) sunt reglementate prin documentul QSIGN-CP-CPS-AC-v1.0. Toate aceste documente sunt publicate în repository-ul oficial al QSIGN și partajează aceeași infrastructură PKI cu Root CA comună.

1.3 Statutul juridic și efectele mărcii temporale calificate

Marca temporală calificată emisă de QSIGN, în calitate de prestator calificat de servicii de încredere înscris în Lista sigură națională (Trusted List) administrată de ADR conform ETSI TS 119 612 și art. 22 din Reg. (UE) 910/2014, beneficiază de prezumțiile prevăzute la art. 41 alin. (2) eIDAS: (a) prezumția de exactitate a datei și orei pe care marca temporală le indică și (b) prezumția de integritate a datelor cu care data și ora sunt asociate. Mai mult, conform art. 41 alin. (3) eIDAS, o marcă temporală calificată emisă într-un stat membru este recunoscută drept marcă temporală calificată în toate celelalte state membre. Aceleași prezumții și efecte sunt confirmate prin art. 6 din Legea nr. 214/2024.

Marca temporală calificată emisă de QSIGN îndeplinește cumulativ cerințele art. 42 alin. (1) eIDAS: (a) leagă data și ora de date într-un mod care exclude în mod rezonabil posibilitatea modificării nedetectabile a datelor; (b) este bazată pe o sursă de timp exactă legată de timpul universal coordonat (UTC); (c) este semnată electronic prin utilizarea unei semnături electronice avansate sau sigilată prin utilizarea unui sigiliu electronic avansat al QSIGN ori printr-o metodă echivalentă.

1.4 Identificarea documentului și OID-uri

1.4.1 Arborele OID QSIGN

QSIGN va opera sub un Private Enterprise Number (PEN) IANA propriu, înregistrat în arborele 1.3.6.1.4.1. Pentru documentele aflate în curs de înregistrare la momentul depunerii dosarului ADR, este utilizat un OID provizoriu în formatul 1.3.6.1.4.1.59019; PEN-ul efectiv va fi înregistrat și actualizat în prezentul document anterior emiterii primei mărci temporale calificate în producție. Arborele OID este partajat cu celelalte servicii QSIGN, ramura .4 fiind rezervată exclusiv serviciilor TSA.

Element	Valoare	Descriere
Arc rădăcină QSIGN	1.3.6.1.4.1.59019	Spațiul OID propriu al QSIGN S.R.L. (PEN provizoriu)
Documente de politică	1.3.6.1.4.1.59019.1	CP, CPS, TSA Policy, T&C, PDS
Politica TSA QSIGN (calificat)	1.3.6.1.4.1.59019.1.4.1	Identificator alocat prezentei politici (QSIGN QTST Policy)

Element	Valoare	Descriere
OID document (versiune)	1.3.6.1.4.1.59019.1.4.1.0	Identificator versiune 1.0 a prezentului document

1.4.2 OID-uri politică ETSI standardizate

Pentru interoperabilitate cu validatorii externi (Adobe AATL, EU LOTL Validator, librării DSS-X, eIDAS Dashboard), fiecare TimeStampToken emis de QSIGN include în câmpul TSTInfo.policy atât OID-ul politicii proprii QSIGN, cât și OID-ul canonic ETSI corespunzător „best-practices QTST", definit în ETSI EN 319 421:

Politică ETSI	OID canonic	Denumire completă
Best-practices QTST	0.4.0.2023.1.1	ETSI EN 319 421 — Time-Stamping Authority best practices for Qualified Time-Stamps
QSIGN QTST Policy	1.3.6.1.4.1.59019.1.4.1	Politica QSIGN aliniată EN 319 421 și art. 42 Reg. (UE) 910/2014

1.5 Documente conexe

Prezenta Politică TSA face parte dintr-un corp documentar coerent al QSIGN, structurat astfel:

- **QSIGN-CP-CPS-QC-v1.0 —** Politica de Certificare și Codul de Practici și Proceduri pentru serviciile calificate de certificat (semnătură QES, sigiliu QESeal, gestiune la distanță cu QSCD).
- **QSIGN-CP-CPS-AC-v1.0 —** Politica de Certificare și Codul de Practici și Proceduri pentru serviciile necalificate (avansate) — certificate AdES sub politicile NCP+, NCP, LCP.
- **ArhitectPKI —** Arhitectura detaliată a serviciului de încredere — ierarhia PKI și politicile sprijinite, document anexat conform art. 5 alin. (2) lit. g) din Anexa 1 la Ordinul MEDAT 102/2026.
- **QSIGN-TSA-PDS —** Time-Stamping Disclosure Statement (PDS) — sumar non-tehnic destinat părților utilizatoare.
- **QSIGN-BCP-DRP —** Plan de continuitate a activității și recuperare în caz de dezastru.
- **QSIGN-TermPlan —** Plan de încetare a activității conform art. 24 alin. (2) lit. (i) din Reg. (UE) 910/2014.
- **QSIGN-IncidentNotif —** Procedura de notificare a incidentelor (ADR, DNSC, ANSPDCP) conform art. 19 alin. (2) eIDAS.

1.6 Convenții de redactare

Termenii englezi sunt utilizați pentru a păstra conformitatea cu vocabularul tehnic standardizat ETSI/IETF; corespondentul în limba română este indicat la prima utilizare. Verbele „trebuie", „este obligat", „va" exprimă cerințe normative; „poate" exprimă facultăți. Trimiterile la articole din Regulamentul (UE) nr. 910/2014 sunt făcute la versiunea consolidată după Reg. (UE) 2024/1183. Trimiterile la standardele ETSI sunt făcute la versiunile în vigoare la data aprobării prezentului document, urmând regula de versiune mobilă („sau ulterioare"), cu evaluare a substanței conformității la auditurile periodice. Termenii „TSA" (Time-Stamping Authority), „TSU" (Time-Stamping Unit), „TST" (TimeStampToken), „TSReq" și „TSResp" au sensurile definite în RFC 3161, RFC 5816 și ETSI EN 319 421.

2. Identificarea politicii și trasabilitatea

2.1 Identificator de politică (policy OID)

Fiecare TimeStampToken emis de QSIGN sub prezenta politică include în câmpul TSTInfo.policy un identificator de obiect (Policy OID) compus, format prin asocierea a doi OID-uri reprezentând politica QSIGN și politica canonică ETSI, în scopul asigurării interoperabilității și al confirmării statutului calificat al serviciului. În caz de conflict de interpretare, OID-ul propriu QSIGN prevalează asupra celui canonic ETSI ca purtător al cerințelor practice particulare ale TSP-ului. Identificatorii sunt:

- **OID politică QSIGN:** `1.3.6.1.4.1.59019.1.4.1` — desemnează prezenta Politică TSA pentru servicii calificate.
- **OID canonic ETSI:** `0.4.0.2023.1.1` — desemnează politica „best-practices QTST" definită în ETSI EN 319 421 §5 și consolidează încadrarea ca QTST în sensul Reg. (UE) 910/2014 art. 42.

2.2 Trasabilitatea cerințelor regulamentare și standardizate

Tabelul de mai jos asigură trasabilitatea exhaustivă între cerințele regulamentare și standardizate aplicabile și secțiunile prezentului document care le implementează. Această trasabilitate facilitează evaluarea conformității de către auditorul Conformity Assessment Body (CAB) acreditat conform Reg. (CE) 765/2008 și de către ADR în calitate de organism de supraveghere conform art. 17 eIDAS.

Cerință	Sursă	Secțiune din prezentul document
Mecanism de legare a datei/orei la date	art. 42(1)(a) eIDAS	§4.1, §6.2 (TSTInfo.messageImprint)
Sursă de timp exactă legată de UTC	art. 42(1)(b) eIDAS	§4.2, §4.3 (surse PTB/NIST/INRIM)

Cerință	Sursă	Secțiune din prezentul document
Semnare prin AdES/sigiliu avansat al TSP	art. 42(1)(c) eIDAS	§4.4, §6.1 (cheia TSU în HSM QSCD-grade)
Notificarea incidentelor (24h)	art. 19(2) eIDAS	§5.6 și document QSIGN-IncidentNotif
Retenție loguri 10 ani	art. 24(2)(h) eIDAS	§4.7, §5.5
Plan de încetare a activității	art. 24(2)(i) eIDAS	§7.4 și document QSIGN-TermPlan
Cerințe generale TSP	ETSI EN 319 401	Întreg documentul, în special §5
Cerințe specifice TSA	ETSI EN 319 421 v1.3.1	Întreg documentul (structură derivată)
Profil TSReq/TSResp	ETSI EN 319 422 v1.1.1; RFC 3161; RFC 5816	§4.4, §6.2
Audit de conformitate	art. 20 eIDAS; ETSI EN 319 403-1	§7.1–§7.3

3. Comunitatea utilizatorilor și aplicabilitate

3.1 Roluri și participanți

Comunitatea care interacționează cu serviciul QSIGN TSA este structurată conform ETSI EN 319 421 §4 (general concepts) în următoarele roluri:

3.1.1 TSA — Time-Stamping Authority

TSA este QSIGN S.R.L., în calitate de prestator calificat de servicii de încredere care își asumă responsabilitatea pentru mărcile temporale calificate emise în prezenta politică. TSA controlează unitatea TSU, gestionează cheia privată a TSU în HSM, asigură sincronizarea cu UTC(k) și păstrează evidențele necesare auditului. TSA exercită funcția prin Policy Management Authority (PMA), care aprobă politicile, procedurile și ceremoniile, precum și prin echipa de exploatare PKI.

3.1.2 TSU — Time-Stamping Unit

TSU desemnează combinația dintre cheia privată dedicată semnării TimeStampToken-urilor, certificatul X.509 corespunzător cheii publice și componenta hardware/software (HSM + serverul TSA) care execută operațiunea de semnare. QSIGN exploatează inițial o singură unitate TSU, denumită „QSIGN TSA Unit G1", al cărei certificat este emis direct de QSIGN Root CA G1 — practică recomandată de ETSI EN 319 421 §7.7.4, întrucât elimină dependența de un Sub-CA emitător și simplifică validarea pe termen lung.

3.1.3 Subscriber

În contextul serviciului TSA, subscriber-ul este însuși QSIGN, întrucât marca temporală nu este emisă pe numele unui utilizator final identificat în certificat. Persoanele și organizațiile care solicită mărci temporale prin protocolul TSReq/TSResp sunt denumite Requesters (solicitanți), iar relația lor cu TSP este reglementată prin Termenii și Condițiile aplicabile (vezi §8).

3.1.4 Requester (solicitant)

Requester-ul este orice persoană fizică sau juridică ce trimite o cerere de marcă temporală (TSReq) către serviciul TSA al QSIGN, prin endpoint-ul oficial publicat în repository. Requester-ul poate fi un utilizator individual, o aplicație de semnare automată (cu sigiliu calificat sau avansat), un sistem de arhivare electronică sau orice altă entitate ce necesită atestarea unui hash la un moment de timp dat. Requester-ul nu este identificat individual în TimeStampToken; identificarea sa, după caz, se face prin mecanisme externe (autentificare API, IP-uri agreate prin contract, prezentare de certificat client TLS) și nu afectează valoarea juridică a TST emisă.

3.1.5 Relying Party (parte utilizatoare)

Relying Party este orice persoană fizică sau juridică ce, în mod rezonabil, se bazează pe o marcă temporală emisă de QSIGN în luarea unei decizii sau efectuarea unei acțiuni — de regulă, în procesul de validare a unei semnături electronice AdES-T sau AdES-LT, în arhivare electronică sau în jurnalizare cu valoare probatorie. Drepturile și obligațiile relying parties sunt detaliate în Capitolul 8 al prezentului document.

3.1.6 ADR și DNSC — autorități naționale

- **ADR — Autoritatea pentru Digitalizarea României** — organism național competent pentru supravegherea prestatorilor calificați conform art. 17 eIDAS și pentru gestionarea Listei sigure (Trusted List) conform art. 22 eIDAS.
- **DNSC — Directoratul Național de Securitate Cibernetică** — autoritatea națională de securitate cibernetică, cu atribuții în Lista Auditorilor de Securitate Cibernetică (LASC) și în managementul incidentelor de securitate.
- **CAB — Conformity Assessment Body** — organism de evaluare a conformității acreditat conform Reg. (CE) 765/2008, care emite raportul de evaluare prevăzut de art. 20 eIDAS și de art. 5 alin. (2) lit. a) din Anexa 1 la Ordinul MEDAT 102/2026.

3.2 Aplicabilitate și utilizări tipice

Marcajele temporale calificate emise de QSIGN sunt destinate următoarelor utilizări tipice:

- **Validare AdES pe termen lung (LTV/LTA):** integrare în profilurile de semnătură AdES-T (Time), AdES-LT (Long Term) și AdES-LTA (Long Term Archival), conform ETSI EN 319 122 (CAdES), EN 319 132 (XAdES), EN 319 142 (PAdES) și EN 319 162 (ASiC).

- **Arhivare electronică:** marcarea temporală a obiectelor de arhivă, în conformitate cu Legea nr. 135/2007 privind arhivarea documentelor electronice și cu cerințele administratorilor de arhivă electronică acreditați.
- **Sigilare temporală API/B2B:** atestarea momentului de generare/recepție a unui mesaj API, eveniment în log-uri cu valoare probatorie, tranzacții EDI.
- **e-Factura și raportări fiscale:** confirmarea momentului de generare a documentelor fiscale electronice ce necesită o cronologie verificabilă.
- **Cronologie pentru proprietate intelectuală:** atestarea anteriorității unei creații (lucrări științifice, software, design, opere de artă) prin marcarea temporală a hash-ului acesteia.

3.3 Utilizări interzise sau nerecomandate

- Utilizarea TimeStampToken-urilor emise de QSIGN ca probe pentru evenimente fizice (de exemplu, momentul exact al unei livrări fizice) — TST atestă doar momentul prelucrării unui hash, nu existența evenimentului asociat.
- Utilizarea endpoint-ului TSA ca sursă oficială de timp pentru sincronizarea de sistem (se vor folosi în acest scop sursele NTP standard ale TSP-ului sau, recomandat, surse stratum-1 NMI publice).
- Utilizarea unui TimeStampToken după revocarea certificatului TSU, dacă revocarea a avut loc înainte de momentul atestat (vezi §6.4 privind regulile de validare în timp).

4. Practicile TSA

4.1 Principii operaționale

QSIGN operează unitatea TSA conform principiilor de la art. 24 alin. (2) lit. (e)–(j) din Reg. (UE) 910/2014, ale ETSI EN 319 401 §7 (Trust Service Provider Practice) și ale ETSI EN 319 421 §6–§7. Principiile fundamentale sunt: (a) sole control asupra cheii TSU prin păstrarea acesteia într-un modul criptografic (HSM) certificat și prin reguli „four-eyes" la operațiunile sensibile; (b) emitere automată, fără intervenție umană în lanțul TSReq → TSU → TSResp; (c) trasabilitate completă a fiecărei mărci temporale emise prin loguri imutabile cu hash-chaining; (d) sincronizare continuă cu UTC(k) și oprire automată a emiterii dacă offset-ul depășește pragul critic.

4.2 Precizia ceasului — cerințe și SLA

Conform ETSI EN 319 421 §7.7.2, marca temporală calificată trebuie să aibă o precizie de cel mult 1 secundă față de UTC. QSIGN se angajează la următoarele niveluri de precizie operațională:

Parametru	Valoare angajată	Mecanism de monitorizare
Precizie absolută (offset UTC)	≤ 1 secundă (cerință legală)	Câmpul TSTInfo.accuracy raportează intervalul efectiv (uzual sub 100 ms)
Precizie țintă operațională	≤ 100 ms (P95)	Monitorizare continuă chrony/ntpq cu metrici offset, jitter, dispersion
Prag de alertă (warning)	> 100 ms	Notificare echipă SOC, investigare automată surse NTP
Prag critic (stop emitere)	> 500 ms	Oprire automată TSU, emitere TSResp granted = false (status: timeNotAvailable) până la re-sincronizare validată
Disponibilitate țintă	99.9% (anual)	Monitorizare uptime, raportare lunară
Latență țintă TSReq → TSResp	≤ 1 secundă (P95)	Monitorizare per-request prin SIEM Wazuh

Implementarea se bazează pe componenta chrony (RFC 5905 / RFC 8915) configurată cu cei trei stratum-1 NMI listați în §4.3, cu algoritm intersection + clustering aplicat pentru excluderea automată a unei surse aberante. Ceasul HSM este sincronizat cu serverul TSA prin canal autentificat. Devierea de fază între ceasul HSM și ceasul UTC este monitorizată continuu prin probe de comparație, cu prag de re-disciplinare la 50 ms.

4.3 Surse de timp UTC(k)

În conformitate cu cerința art. 5 alin. (2) lit. u) din Anexa 1 la Ordinul MEDAT 102/2026 și cu cerințele ETSI EN 319 421 §7.7.2, QSIGN utilizează trei surse stratum-1 NTP gestionate de Institute Naționale de Metrologie (NMI), trasabile la UTC(k) și listate de Bureau International des Poids et Mesures (BIPM). Sursele sunt diverse geografic, asigurând redundanță conformă cerințelor BCP/DRP:

Sursă	Rol	Servere stratum-1 / observații
PTB (Germania)	Primar	Physikalisch-Technische Bundesanstalt — ptbtime1.ptb.de, ptbtime2.ptb.de, ptbtime3.ptb.de, ptbtime4.ptb.de — trasabilitate UTC(PTB), suport NTP + Network Time Security (NTS, RFC 8915).
NIST (SUA)	Secundar	National Institute of Standards and Technology — time.nist.gov, time-a-g.nist.gov, time-b-

Sursă	Rol	Servere stratum-1 / observații
		g.nist.gov — trasabilitate UTC(NIST), suport NTP cu autentificare prin cheie simetrică (la cerere); diversitate geografică transatlantică.
INRIM (Italia)	Terțiar	Istituto Nazionale di Ricerca Metrologica — ntp1.inrim.it, ntp2.inrim.it — trasabilitate UTC(IT), NMI european alternativ pentru DR/BCP.

Două servere interne stratum-2 (chrony, configurate redundant pe noduri Proxmox separate) consumă cele trei surse, aplică algoritmul intersection + clustering definit în RFC 5905 §11 pentru detectarea și excluderea automată a unei surse aberante (falseticker), și disemnează timpul către serverul TSA și către ceasul HSM. Configurația și auditul de sincronizare sunt detaliate în documentul „Arhitectura detaliată a serviciului de încredere", §9.

4.4 Profilul protocolului TSA (TSReq / TSResp)

Protocolul TSA implementează RFC 3161 (Time-Stamp Protocol) cu extensia ESSCertIDv2 conform RFC 5816 și profilul de transport ETSI EN 319 422 v1.1.1 (HTTPS POST cu Content-Type application/timestamp-query, răspuns application/timestamp-reply).

4.4.1 Profilul TSReq (Time-Stamp Request)

QSIGN acceptă cereri TSReq cu următoarele caracteristici:

- **version:** 1 (RFC 3161 §2.4.1).
- **messageImprint.hashAlgorithm:** id-sha256 (1.2.840.113549.1.1.11) — algoritm implicit; opțional id-sha384 (1.2.840.113549.1.1.12) sau id-sha512. Algoritmii sha-1 și md5 sunt explicit refuzați (TSResp granted = false, status: badAlg).
- **messageImprint.hashedMessage:** octet string de lungime fixă conform algoritmului (32B pentru SHA-256, 48B pentru SHA-384, 64B pentru SHA-512).
- **reqPolicy:** opțional; dacă este prezent, trebuie să fie 1.3.6.1.4.1.59019.1.4.1 (QSIGN QTST) sau 0.4.0.2023.1.1 (best-practices QTST). În caz de mismatch, TSResp granted = false, status: unacceptedPolicy.
- **nonce:** opțional, dar recomandat (anti-replay); valoarea se reflectă în TSTInfo.nonce.
- **certReq:** boolean; dacă TRUE, TSResp include certificatul TSU (recomandat pentru relying parties care nu au acces la AIA).
- **extensions:** nu sunt suportate la momentul aprobării prezentei politici; orice extensie marcată critical va determina respingerea cererii.

4.4.2 Profilul TSResp (Time-Stamp Response)

TSResp constă în două componente: status (PKIStatusInfo) și timeStampToken. Statusurile întoarse de QSIGN sunt:

PKIStatus	PKIFailureInfo	Semnificație
granted (0)	—	TimeStampToken emis cu succes, fără modificări asupra cererii.
grantedWithMods (1)	—	TimeStampToken emis cu o politică/algoritm modificate; QSIGN nu utilizează în practică acest status.
rejection (2)	badAlg	Algoritm de hash nesuportat (sha-1, md5).
rejection (2)	badRequest	Cerere malformată sau cu câmpuri invalide.
rejection (2)	badDataFormat	messageImprint.hashedMessage de lungime incorectă pentru algoritmul indicat.
rejection (2)	timeNotAvailable	Sursa de timp este indisponibilă sau offset > 500 ms (vezi §4.2).
rejection (2)	unacceptedPolicy	reqPolicy nu corespunde politicilor sprijinite.
rejection (2)	unacceptedExtension	Extensie critică nesuportată în TSReq.
rejection (2)	systemFailure	Eroare internă; incident raportat conform §5.6.
waiting (3)	—	Nu este utilizat de QSIGN — emitere sincronă.

4.4.3 Profilul TSTInfo (TimeStampToken)

TimeStampToken-ul este structurat conform RFC 3161 §2.4.2 și RFC 5816 (extensia ESSCertIDv2):

Câmp TSTInfo	Conținut
version	v1 (= 1)
policy	OID compus: 1.3.6.1.4.1.59019.1.4.1 (QSIGN QTST) împreună cu 0.4.0.2023.1.1 (best-practices QTST), conform §2.1
messageImprint	preluat identic din TSReq — hashAlgorithm și hashedMessage
serialNumber	număr unic, monotonic, pe minimum 64 biți de entropie criptografică din HSM (RFC 3161 §2.4.2)
genTime	timp UTC, format GeneralizedTime cu precizie microsecundă (Z-suffixed)
accuracy	≤ 1 secundă (raportat în practică în microsecunde, conform §4.2)
ordering	FALSE (genTime asigură singur ordonarea cronologică)

Câmp TSTInfo	Conținut
nonce	preluat din TSReq dacă a fost prezent (anti-replay)
tsa	GeneralName tip directoryName cu DN-ul TSU
extensions	nu sunt utilizate în prezenta versiune a politicii

TimeStampToken-ul este împachetat ca un SignedData CMS (RFC 5652) semnat cu cheia TSU. Atributele semnate obligatorii includ contentType (id-ct-tstInfo), messageDigest (peste TSTInfo encodat DER) și signingCertificateV2 cu hash SHA-256 conform RFC 5816 (eliminând astfel dependența de certificate trecute prin SHA-1 din profilul original RFC 3161).

4.5 Algoritmi criptografici și parametri

QSIGN aplică recomandările ETSI TS 119 312 v1.5.1 (Cryptographic Suites) și SOG-IS Agreed Cryptographic Mechanisms v1.3, în măsura în care intră în referința art. 8 alin. (3) din Reg. (UE) 910/2014. Configurația minimă acceptată în 2026:

Componentă	Algoritm / parametri	Standard / observație
Cheie TSU	RSA-4096 sau ECDSA P-384	ETSI TS 119 312 §5.1.6; SOG-IS Higher
Algoritm semnătură TSU	sha256WithRSAEncryption (default) sau ecdsa-with-SHA384	RFC 5652
Hash messageImprint suportat	SHA-256, SHA-384, SHA-512	RFC 3161; ETSI EN 319 422
Hash messageImprint refuzat	SHA-1, MD5	depreciate, badAlg
signingCertificateV2 hash	SHA-256	RFC 5816
Generator aleatoriu (serialNumber, nonce)	DRBG NIST SP 800-90A din HSM	FIPS 140-2 §4.7
TLS pentru endpoint TSA	TLS 1.2/1.3 cu suite AEAD (ECDHE-RSA-AES-GCM, ECDHE-ECDSA-CHACHA20)	BSI TR-02102-2 / SOG-IS

4.6 Managementul cheii TSU

4.6.1 Generarea cheii TSU

Cheia privată TSU este generată în interiorul HSM-ului calificat (Common Criteria EAL4+ / FIPS 140-2 nivel 3, listat în Lista QSCD UE), prin ceremonie planificată, cu prezența a cel puțin doi membri ai PMA, a Security Officer-ului și, opțional, a unui auditor extern.

Ceremonia respectă procedura de cheie m-of-n (3 din 5 deținători de smart cards de activare). Activitățile sunt înregistrate video, documentate într-un Key Ceremony Record semnat olograf de toți participanții și păstrate în arhiva fizică minimum 10 ani.

4.6.2 Protecția cheii TSU

Cheia privată TSU este nemobilă: nu poate fi exportată în clar din HSM. Operațiunile de semnare TimeStampToken sunt realizate exclusiv în interiorul modulului criptografic, prin canal PKCS#11 autentificat. Două HSM-uri Thales Luna (sau echivalent Utimaco SecurityServer) operează în cluster activ-pasiv, cu replicare a cheii prin mecanismul nativ al producătorului (key cloning protejat criptografic). Backup-ul cheii este wrapped (cifrat cu o cheie KEK separată), păstrat în două locații geografice distincte, activabil doar prin cvorum 3-of-5 al deținătorilor de smart cards.

4.6.3 Validitatea și ciclul de viață

Certificatul TSU are o perioadă de validitate de 5 ani (renoibilă), cu rotație planificată la 4 ani și o perioadă de overlap de 12 luni. La sfârșitul perioadei de utilizare, cheia privată este distrusă criptografic conform NIST SP 800-88 Rev. 1 (zeroizare HSM cu certificat de distrugere). Certificatul TSU este menținut în repository pentru permite validarea a posteriori a TimeStampToken-urilor emise în timpul perioadei sale de validitate. Detalii despre formatul și extensiile certificatului TSU sunt date în §6.1.

4.6.4 Revocarea cheii / certificatului TSU

Certificatul TSU poate fi revocat în următoarele cazuri excepționale: (a) compromiterea suspectată sau confirmată a cheii private (keyCompromise); (b) defectarea HSM-ului fără posibilitate de recuperare a cheii (cessationOfOperation); (c) modificarea politicii TSA cu impact asupra emiterii (superseded); (d) încetarea activității TSP-ului. Decizia de revocare este luată de PMA, semnată de Administratorul QSIGN și executată prin ceremonie de revocare la nivelul Root CA (care emite un nou CRL incluzând certificatul TSU revocat). În cazul revocării, QSIGN notifică ADR în maximum 24 ore conform art. 19 alin. (2) eIDAS, publică anunțul de revocare în repository și transmite notificare către relying parties cunoscute. Trust List națională va fi actualizată corespunzător prin ADR.

4.7 Logurile de audit și retenția

Conform art. 24 alin. (2) lit. (h) din Reg. (UE) 910/2014, QSIGN păstrează toate informațiile relevante referitoare la datele emise și primite, inclusiv mărcile temporale calificate emise, pe o perioadă minimă de 10 ani de la încetarea activității TSP. Pentru serviciul TSA, evenimentele înregistrate include:

- Fiecare TSReq primit (timestamp recepție, IP sursă, lungime, hash inputului, dimensiune, statusul de procesare).
- Fiecare TSResp emis (PKIStatus, PKIFailureInfo dacă rejection, serialNumber al TimeStampToken-ului, hash al TST).

- Toate evenimentele de operare a HSM-ului (login, logout, operațiuni cu cheia TSU, alarme).
- Sincronizarea cu sursele NTP — offset, jitter, dispersion, evenimente de re-disciplinare, evenimente de stepping.
- Ceremoniile de cheie (generare, backup, recovery, retragere).
- Accesări privilegiate la sistem (administratori, auditori) și modificări de configurație.
- Incidente de securitate și operare, conform §5.6.

Logurile sunt agregate prin Wazuh Manager, transportate prin rsyslog cu TLS, semnate periodic cu o cheie dedicată de audit (hash chaining peste blocuri orare) și exportate într-un sistem WORM (Write-Once-Read-Many). În plus, QSIGN are contract cu un administrator de arhivă electronică acreditat conform Legii nr. 135/2007 pentru conservarea pe termen lung a evidenței mărcilor temporale și a logurilor de audit.

Datele cu caracter personal eventual incluse în loguri (de exemplu, IP-uri, identificatoare de aplicație) sunt prelucrate pe temeiul art. 6 alin. (1) lit. (c) GDPR (obligație legală — eIDAS art. 24 alin. (2) lit. (h)) și art. 6 alin. (1) lit. (f) (interes legitim — securitatea serviciului). Detalii despre prelucrare sunt în notificarea de informare GDPR a QSIGN.

5. Securitate fizică, logică și organizațională

5.1 Cadru general

Securitatea TSA este parte integrantă a Sistemului de Management al Securității Informației (ISMS) al QSIGN, organizat conform ISO/IEC 27001 și ETSI EN 319 401. Sistemul informatic care susține TSA este organizat în patru zone de securitate cu segmentare logică (firewall L7) și fizică (cabinete dedicate, separare alimentare), aplicând principiul defense-in-depth: (i) zona publică (Internet — abonați, relying parties), (ii) DMZ (frontend, reverse-proxy/WAF, OCSP, CRL/AIA), (iii) zona de securitate înaltă (TSP backend — TSA Server, RA Backend, HSM LAN, SIEM), (iv) zona offline (Root CA, HSM Root, backup KMS, arhivă long-term). Tranzițiile între zone sunt strict controlate; transferul în/din zona offline se face exclusiv pe suport detașabil în cadrul ceremoniilor înregistrate.

5.2 Securitatea fizică

Echipamentele care găzduiesc TSU și HSM-urile aferente sunt instalate într-un centru de date cu următoarele controale:

- Acces controlat cu multi-factor (badge + biometrie + PIN), cu evidență centralizată și retenție 10 ani.
- Supraveghere video continuă cu retenție minim 90 zile (recomandat 180 zile pentru centre de înaltă securitate).
- Zone delimitate (perimetric, recepție, sală operatori, cabinet HSM, cabinet Root CA offline) cu controale crescătoare.

- Detectare incendiu cu suprimare cu gaz inert (FM-200 sau echivalent), fără afectarea echipamentelor.
- Alimentare redundantă (UPS + generator) cu autonomie minimum 24h și SLA de mentenanță continuă.
- Climatizare redundantă, monitorizată de senzori cu alertare în SOC.
- Cabinet Root CA în air-gap fizic, deschis doar la ceremonii cu prezența cvorumului PMA și înregistrare video.

5.3 Securitatea logică

Configurația de securitate logică aplicată sistemelor TSA include:

- **Hardening:** OS minimal (Debian 12 stable; Buildroot pentru dispozitive specializate), kernel hardenat (lockdown=integrity, modules signed-only), SELinux în mod enforcing pentru CA online și TSA, nftables ca firewall L7 cu reguli explicite per serviciu.
- **Autentificare administratori:** autentificare cu factor multiplu obligatorie (smart-card eIDAS QSCD + parolă + cod TOTP); sesiunile administrative sunt înregistrate audio-video și auditate.
- **Principiul „4-eyes":** orice operațiune cu impact asupra cheilor TSA, asupra politicilor de emitere sau asupra surselor de timp necesită aprobarea a doi administratori distincți cu roluri separate.
- **Separarea atribuțiilor:** rolurile de Security Officer, PKI Operator, Auditor Intern și DPO sunt incompatibile între ele; un membru PMA nu poate cumula concomitent funcția de auditor extern al aceluiași serviciu.
- **Patch management:** aplicarea patch-urilor critice de securitate în maxim 7 zile de la publicare, cu testare prealabilă în mediu de staging.
- **Detection & Response:** IDS/IPS (Suricata cu Emerging Threats Pro), SIEM (Wazuh Manager), monitorizare 24/7 prin SOC propriu sau partener contractat.

5.4 Personal și organizare

QSIGN aplică o politică de personal aliniată ETSI EN 319 401 §7.2 (personnel security):

- Toate persoanele care interacționează cu TSA semnează acord de confidențialitate și sunt verificate prin background check (cazier judiciar, verificare referințe profesionale).
- Pregătirea inițială și refresher anual pe teme de securitate, eIDAS, ETSI EN 319 401, GDPR.
- Roluri de încredere (Trusted Roles) clar definite și documentate: PMA Members, Security Officer, PKI Operator (TSA Operator), System Administrator, Internal Auditor, DPO.
- Plan de succesiune pentru toate rolurile critice; documentație runbook sufficientă pentru continuitate.

- Procedura de „off-boarding" la încetarea contractului: revocare imediată a accesurilor, returnare echipamente și smart cards, păstrarea acordului de confidențialitate post-contract minimum 3 ani.

5.5 Logging și audit intern

Pe lângă logurile descrise în §4.7, QSIGN menține un program de audit intern:

- Audit intern cel puțin anual al sistemului ISMS, cu raport scris către PMA.
- Audit anual al ceremoniei de cheie și al backup-urilor cripto, cu test de restaurare validat.
- Reviziri trimestriale ale logurilor de audit pentru identificarea anomaliilor de tendință.
- Test de penetrare (pentest) anual, cu remediere a vulnerabilităților critice și majore în maximum 30 zile.
- Test BCP/DRP anual cu scenariu realistic (failure HSM primar, pierdere centru de date primar, indisponibilitate surse NTP).

5.6 Managementul incidentelor

În caz de incident de securitate sau compromis, QSIGN urmează procedura documentată în QSIGN-IncidentNotif:

- **Detectare și triaj:** SOC analizează alerta, încadrează severitatea (P1–P4) și escaladează către Security Officer pentru P1/P2.
- **Notificare ADR:** în maxim 24 ore conform art. 19 alin. (2) eIDAS, prin canal securizat (e-mail semnat cu sigiliu calificat la incident@adr.gov.ro).
- **Notificare ANSPDCP:** în maxim 72 ore conform art. 33 GDPR, dacă incidentul implică date cu caracter personal.
- **Notificare DNSC:** conform Legii nr. 58/2023 (NIS2), pentru incidente cu impact semnificativ asupra serviciilor de încredere.
- **Notificare relying parties:** publicare anunț în repository QSIGN și, după caz, notificare directă către abonații care ar putea fi afectați.
- **Containment, eradication, recovery:** aplicare măsuri imediate (revocare TSU, oprire emitere), curățare cauză rădăcină, restaurare serviciu.
- **Lessons learned:** post-mortem documentat, comunicat PMA și auditorului, cu plan de acțiune pentru prevenirea reapariției.

6. Profilul certificatului TSU și al TimeStampToken

6.1 Profilul certificatului TSU (X.509 v3)

Certificatul TSU este un certificat X.509 v3 emis direct de QSIGN Root CA G1 (a se vedea §3 din documentul „Arhitectura detaliată a serviciului de încredere"). Această practică, recomandată de ETSI EN 319 421 §7.7.4, elimină dependența unui Sub-CA emitător și

simplifică validarea pe termen lung. Profilul certificatului TSU este aliniat ETSI EN 319 412-1/-2:

Câmp / Extensie	Conținut
version	3 (v3)
serialNumber	număr aleatoriu, minimum 64 biți de entropie din HSM Root CA
signature	sha384WithRSAEncryption (OID 1.2.840.113549.1.1.12) — semnată de Root CA
issuer	CN = QSIGN Root CA G1, O = QSIGN S.R.L., OID 2.5.4.97 = VATRO-34633481, C = RO
validity	5 ani (Not Before / Not After în GeneralizedTime UTC)
subject	CN = QSIGN TSA Unit G1, O = QSIGN S.R.L., OID 2.5.4.97 = VATRO-34633481, C = RO, serialNumber = TSU-G1-001
subjectPublicKeyInfo	rsaEncryption — RSA-4096 (SHA-256/384) sau ecPublicKey — ECDSA P-384
KeyUsage (CRITICAL)	digitalSignature, nonRepudiation (contentCommitment) — exact aceste două bituri
ExtendedKeyUsage (CRITICAL)	id-kp-timeStamping (1.3.6.1.5.5.7.3.8) — extensie marcată critică, EXCLUSIV (fără alte EKU)
certificatePolicies	1.3.6.1.4.1.59019.1.4.1 (QSIGN QTST) și 0.4.0.2023.1.1 (best-practices QTST), cu PolicyQualifiers (CPS URI și UserNotice)
CRLDistributionPoints	http://crl.qsign.ro/QSIGN-RootCA-G1.crl
AuthorityInfoAccess	OCSP: http://ocsp.qsign.ro; caIssuers: http://aia.qsign.ro/QSIGN-RootCA-G1.crt
AuthorityKeyIdentifier	KeyId al Root CA
SubjectKeyIdentifier	KeyId derivat din SubjectPublicKey (SHA-1 sau SHA-256 conform RFC 5280)
BasicConstraints	cA = FALSE
qcStatements (informativ)	qcStatement-1 (esi4-qcStatement-1), QcCompliance, QcType id-etsi-qct-eseal (TSU este sigiliu calificat al TSP, conform interpretării art. 42(1)(c) eIDAS)

Marcajul critical pe ExtendedKeyUsage = id-kp-timeStamping este obligatoriu (RFC 3161 §2.3 și ETSI EN 319 422 §6.1) — asigurând că validatorii care nu cunosc semantica timestamping refuză utilizarea cheii TSU pentru alte scopuri (semnătură document, autentificare TLS etc.).

6.2 Profilul TimeStampToken (TST)

Profilul TimeStampToken este detaliat în §4.4.3. Reluăm aici elementele esențiale, cu accent pe cerințele de validare:

- TST este împachetat ca SignedData CMS (RFC 5652), cu eContentType = id-ct-tstInfo (1.2.840.113549.1.9.16.1.4) și eContent conținând TSTInfo encodat DER.
- Atributele semnate obligatorii includ contentType, messageDigest și signingCertificateV2 (RFC 5816), cu ESSCertIDv2 conținând hash SHA-256 al certificatului TSU.
- Atributul signingCertificateV2 elimină dependența SHA-1 din profilul original RFC 3161, conform recomandărilor ETSI EN 319 422 v1.1.1 §6.2.
- Atributul certificate al SignedData include certificatul TSU (dacă TSReq.certReq = TRUE) — recomandat pentru a permite validarea de către relying parties care nu au acces la AIA.
- Atributul crls al SignedData NU este utilizat la emitere (validatorii obțin CRL din CRLDistributionPoints sau prin OCSP).

6.3 Reguli de validare a TimeStampToken

O parte care se bazează (relying party) validează un TimeStampToken emis de QSIGN urmând regulile ETSI EN 319 102-1 (procedurile de validare DSS-X) și RFC 3161 §2.4.2:

- Verifică integritatea TST prin verificarea semnăturii CMS cu cheia publică din certificatul TSU.
- Verifică lanțul de certificate de la TSU până la o ancoră de încredere (QSIGN Root CA G1, prezent în Trust List ADR / EU LOTL).
- Verifică statusul certificatului TSU la momentul atestat (genTime), folosind CRL sau OCSP. Certificatul trebuie să fi fost valid și non-revocat la momentul genTime.
- Verifică messageImprint: hash-ul calculat asupra documentului trebuie să fie identic cu cel din TSTInfo.messageImprint.
- Verifică OID-ul politicii: TSTInfo.policy trebuie să fie 1.3.6.1.4.1.59019.1.4.1 sau 0.4.0.2023.1.1 (sau să le includă pe ambele).
- Verifică precizia: TSTInfo.accuracy trebuie să fie ≤ 1 secundă (cerință legală art. 42 eIDAS).
- (Opțional, pentru anti-replay) Verifică nonce: TSTInfo.nonce trebuie să fie identic cu cel transmis în TSReq.

6.4 Validitatea pe termen lung (LTV/LTA)

Pentru păstrarea valorii probatorii a unei mărci temporale calificate dincolo de durata de viață a certificatului TSU sau a algoritmilor criptografici utilizați, relying parties și subscribers sunt încurajați să aplice strategii de prezervare conforme ETSI EN 319 102-1 §5 și ETSI TS 119 511 / 119 512:

- **Re-time-stamping (TSU re-issue):** aplicarea unei noi mărci temporale calificate (cu o cheie/algoritm mai puternic) peste TST original și restul probelor de validare, pentru a extinde lanțul de încredere.
- **Archival via TSP-uri calificate de prezervare:** utilizarea unui Qualified Preservation Service for Qualified Electronic Signatures/Seals (QPreserveQES, art. 34 eIDAS), care preia responsabilitatea integrității pe termen lung.
- **Trust List a TSP-ului care a încetat activitatea:** chiar și după încetare, ADR păstrează istoric Trust List anterioare, permițând relying parties să valideze TST emise în timpul activității.

7. Audit și conformitate

7.1 Cadrul legal al evaluării de conformitate

În calitate de prestator de servicii de încredere calificate, QSIGN se supune evaluării de conformitate prevăzute la art. 20 alin. (1) și art. 21 alin. (2) din Regulamentul (UE) nr. 910/2014. Evaluarea este realizată de un Conformity Assessment Body (CAB) acreditat conform Reg. (CE) 765/2008 pentru standardul ETSI EN 319 403-1 v2.3.1 (Trust Service Provider Conformity Assessment — Requirements for conformity assessment bodies assessing Trust Service Providers). Raportul de evaluare a conformității constituie anexă obligatorie la dosarul de notificare depus la ADR, conform art. 5 alin. (2) lit. a) din Anexa 1 la Ordinul MEDAT nr. 102/29.01.2026.

7.2 Frecvența și sfera auditului

- **Audit inițial:** înainte de începerea activității, acoperind evaluarea completă a conformității cu ETSI EN 319 401, EN 319 421 și standardele asociate, conform ETSI EN 319 403-1.
- **Audit de supraveghere:** cel puțin la fiecare 24 de luni, conform art. 20 alin. (1) eIDAS — la cerere ADR sau pentru menținerea statutului calificat.
- **Audit de re-evaluare:** la modificări semnificative ale arhitecturii, politicilor sau setului de servicii prestate (de exemplu, înlocuirea HSM, schimbarea Root CA, introducerea unei noi unități TSU).
- **Audit ad-hoc:** la solicitarea ADR, în caz de incident sau plângere fundamentată.

7.3 Sfera materială a auditului TSA

Auditul de conformitate al serviciului TSA acoperă, fără a se limita la, următoarele zone:

- Conformitatea cu cerințele eIDAS (art. 19, 24, 41, 42) și cu Legea 214/2024.
- Conformitatea cu ETSI EN 319 401 §5–§7 și ETSI EN 319 421 §6–§7.
- Conformitatea profilurilor TSReq/TSResp/TSTInfo cu RFC 3161, RFC 5816, ETSI EN 319 422.

- Funcționarea practică a sincronizării cu UTC(k) — măsurători efective ale offset-ului în condiții normale și degradate.
- Verificarea HSM-urilor și a certificărilor (CC EAL4+ / FIPS 140-2 nivel 3, listare în Lista QSCD UE).
- Auditul logurilor de operare TSA pe o perioadă reprezentativă (minimum 6 luni anterioare).
- Auditul ceremoniei de generare/backup a cheii TSU (proces, documentație, înregistrări video, semnături olografe).
- Verificarea procedurilor de notificare a incidentelor și a testelor BCP/DRP.

7.4 Plan de încetare a activității (Termination Plan)

Conform art. 24 alin. (2) lit. (i) din Reg. (UE) 910/2014 și ETSI EN 319 421 §6.12, QSIGN menține un Plan de încetare a activității (Termination Plan) — document distinct (cod QSIGN-TermPlan) — care prevede:

- Notificarea ADR cu cel puțin 90 zile înainte de încetarea planificată a activității.
- Notificarea relying parties cunoscute prin canal direct și prin publicare în repository.
- Transferul responsabilităților către un alt TSP calificat (TSP succesor), dacă este disponibil și acceptat.
- Asigurarea continuității validării TimeStampToken-urilor emise: certificatele TSU și CRL-urile rămân disponibile prin contractul cu administratorul de arhivă electronică pentru minimum 10 ani după încetare.
- Distrugerea criptografică a cheilor TSU (zeroization HSM cu certificat de distrugere).
- Predarea logurilor de audit către ADR sau către administratorul de arhivă electronică agreat.
- Constituirea garanției financiare conform art. 5 alin. (2) lit. b) din Anexa 1 la Ordinul MEDAT 102/2026 (poliță 500.000 EUR per serviciu) pentru acoperirea eventualelor răspunderi post-încetare.

7.5 Modificări ale politicii și ale CPS

Modificările prezentei Politici TSA urmează procedura PMA descrisă în QSIGN-CP-CPS-QC-v1.0 §1.5. Pentru orice modificare substanțială (schimbare de algoritm criptografic, schimbare arhitectură TSU, schimbare procedură de sincronizare cu UTC), QSIGN notifică ADR cu cel puțin 30 zile înainte de intrarea în vigoare, conform art. 9 alin. (2) din Anexa 1 la Ordinul MEDAT 102/2026. Documentul actualizat este publicat în repository, sigilat electronic cu sigiliu calificat al QSIGN și marcat temporal calificat (potențial cu propriul TSU, sub o cheie distinctă), însoțit de un changelog și de OID-ul nou alocat versiunii.

8. Termeni și condiții pentru requesters și relying parties

8.1 Obligațiile QSIGN ca TSA

QSIGN, în calitate de TSP calificat, se obligă față de utilizatorii serviciului TSA:

- Să emită mărci temporale calificate conform art. 42 eIDAS și prezentei politici, cu precizia ≤ 1 secundă față de UTC.
- Să mențină disponibilitatea serviciului la cel puțin 99.9% anual, cu oprirea automată a emiterii doar în cazurile prevăzute la §4.2 (offset > 500 ms).
- Să publice și să mențină actualizate certificatul TSU, CRL-ul aplicabil, prezenta Politică TSA și PKI Disclosure Statement (PDS).
- Să notifice ADR și relying parties despre orice incident cu impact semnificativ în termenele legale (24 ore către ADR, 72 ore către ANSPDCP dacă datele personale sunt afectate).
- Să mențină asigurarea de răspundere civilă în valoare de minim 500.000 EUR pentru serviciul TSA, conform art. 5 alin. (2) lit. b) din Anexa 1 la Ordinul MEDAT 102/2026.
- Să respecte cerințele GDPR (Reg. 2016/679) în prelucrarea oricăror date cu caracter personal asociate operării serviciului.
- Să se supună auditurilor periodice și ad-hoc realizate de CAB-uri acreditate și de ADR.

8.2 Obligațiile requester-ului

Persoana sau aplicația care solicită o marcă temporală (requester) se obligă:

- Să transmită cereri TSReq conforme cu profilul descris la §4.4.1 (algoritmi suportați, structură corectă).
- Să nu utilizeze serviciul în scopuri ilicite sau abuzive (de exemplu, atacuri DoS prin inundare cu cereri).
- Să respecte limitele de utilizare prevăzute în acordul comercial (rate limit, volum maxim) sau în Termenii și Condițiile publicate, după caz.
- Să nu pretindă că un TimeStampToken atestă altceva decât existența unui hash la un moment de timp dat — conform art. 42 eIDAS.
- Să notifice QSIGN dacă observă comportament anormal al serviciului (timestamp-uri cu offset suspect, semnături invalide).

8.3 Obligațiile relying party

Partea utilizatoare a unui TimeStampToken emis de QSIGN se obligă:

- Să verifice TST conform regulilor de validare descrise la §6.3, ca premisă a oricărei decizii bazate pe acesta.
- Să verifice că certificatul TSU este în Trust List națională (TSL administrată de ADR) sau în EU LOTL la momentul de validare.

- Să verifice că certificatul TSU nu era revocat la momentul atestat (genTime), folosind CRL sau OCSP.
- Să nu se bazeze exclusiv pe TST pentru evenimente care necesită forme suplimentare de probă (de exemplu, identitatea unui semnatar — care necesită un certificat calificat de semnătură).
- Să aplice strategii de prezervare (re-time-stamping, QPreserve) pentru valoare probatorie pe termen foarte lung, conform §6.4.

8.4 Limitări de răspundere

QSIGN răspunde pentru daunele cauzate prin neîndeplinirea cu intenție sau din neglijență a obligațiilor sale ca TSP calificat, conform art. 13 din Reg. (UE) nr. 910/2014. Sarcina probei revine: (a) reclamantului, pentru intenția sau neglijența unui TSP non-calificat; (b) TSP-ului calificat (QSIGN), pentru a dovedi că nu a acționat cu intenție sau neglijență, conform art. 13 alin. (2) eIDAS.

Răspunderea financiară a QSIGN este acoperită prin polița de asigurare de răspundere civilă în valoare de 500.000 EUR per serviciu calificat (art. 5 alin. (2) lit. b) din Anexa 1 la Ordinul MEDAT 102/2026), cesionată în favoarea ADR. QSIGN nu răspunde pentru: (i) utilizarea TST în afara sferei de aplicare descrise la §3.2 sau pentru utilizările interzise de la §3.3; (ii) imposibilitatea relying party-ului de a verifica TST din cauza propriilor configurații de sistem; (iii) daune indirecte (lucrum cessans), profit nerealizat sau pierdere de oportunitate, în limita permisă de lege.

8.5 Soluționarea litigiilor

Litigiile rezultate din utilizarea serviciului TSA pot fi soluționate: (a) amiabil, prin notificarea QSIGN la incident@qsign.ro, cu termen de răspuns 30 zile lucrătoare; (b) prin sesizarea ADR în calitate de organism național de supraveghere, conform art. 17 eIDAS; (c) prin instanțele judecătorești române competente material și teritorial, conform normelor de drept comun. Pentru chestiuni privind protecția datelor cu caracter personal, persoana vizată se poate adresa ANSPDCP conform art. 77 GDPR.

8.6 Disponibilitatea informației

Toate documentele relevante pentru utilizatori (prezenta Politică TSA, PKI Disclosure Statement, profil certificat TSU, CRL Root CA, Termenii și Condițiile, Trust List națională) sunt publicate în repository-ul QSIGN la https://www.qsign.ro/repository, în format PDF semnat cu sigiliu calificat al QSIGN și marcat temporal calificat. Endpoint-ul TSA este publicat la https://tsa.qsign.ro/timestamp și este disponibil 24/7. Endpoint-ul OCSP pentru certificatul TSU este http://ocsp.qsign.ro. Versiunile anterioare ale prezentei politici rămân disponibile public minimum 10 ani de la data înlocuirii, în vederea valorii probatorii a TST emise sub politicile anterioare.

Întocmit și certificat,

QSIGN S.R.L. — prin Administrator Trandafirescu Alexandru Florin

Data: 06.05.2026

Semnătura electronică calificată:

_____